

How to Train your Snapdragon

exploring power frameworks on android



A story of Research by:

Josh “m0nk” Thomas / @m0nk_dot

syscan 2014

Is there anyone here from
Qualcomm or Sony?



this hour, your talking head is...

- ❖ Josh “m0nk” Thomas

- ❖ @m0nk_dot
- ❖ Partner and Chief Breaking Officer @ Atredis Partners
- ❖ Recovering software developer (AI / Crypto / Mobile “stuff”)

- ❖ Atredis Partners

- ❖ Focused and targeted security firm
- ❖ Specializing in advanced hardware and software assessments
 - ❖ Mobile and embedded systems
 - ❖ Societal infrastructure
 - ❖ Black boxes
 - ❖ Advanced malware and rootkit analysis
- ❖ Handcrafted artisanal and deep bespoke research



exploring the android kernel is my happy place





@m0nk_dot likes to put
trite commentary in
front of pretty pictures

An aside about malware and rootkits

- ❖ We tend to assume all malware is boring and driven by capitalist intents
- ❖ This mentality changes drastically when we shift our focus to highly advanced and expensive tools
- ❖ I urge you to explore and extend advanced research in the field, there are not enough of us pushing the boundaries in an open manner
- ❖ I open source in an attempt to nullify the use of my research as a weapon



I have no right to use
these pics... sorry :/

story arc



- ❖ story[0] = “hacking assumptive design”
- ❖ story[1] = “Universal Exploitation we can talk about”
- ❖ story[2] = “New study finds that unsafe hardware is unsafe, also hardware”
- ❖ story[3] = “Thank you and further memes”



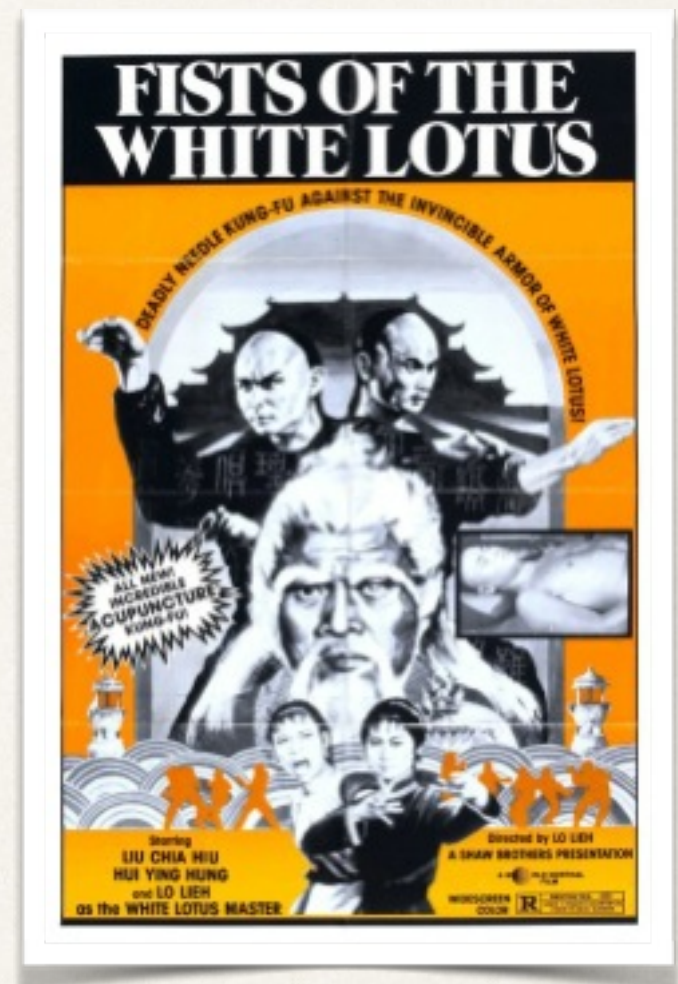
A quick story about assumptive design

with a little help from:



The symbiotic nature of Grey beards & n00bs

- * Grey beards are needed and solve hard problems in known ways
 - * Actual knowledge transferred
 - * Incorrect assumptions transferred as knowledge
- * n00bs are needed to challenge grey beards with new ideas
 - * NOT all new ideas are good ideas
 - * NOT all new ideas are bad ideas
- * “Disruptive Thought” + “Deep Understanding” == “Potential Innovation” *



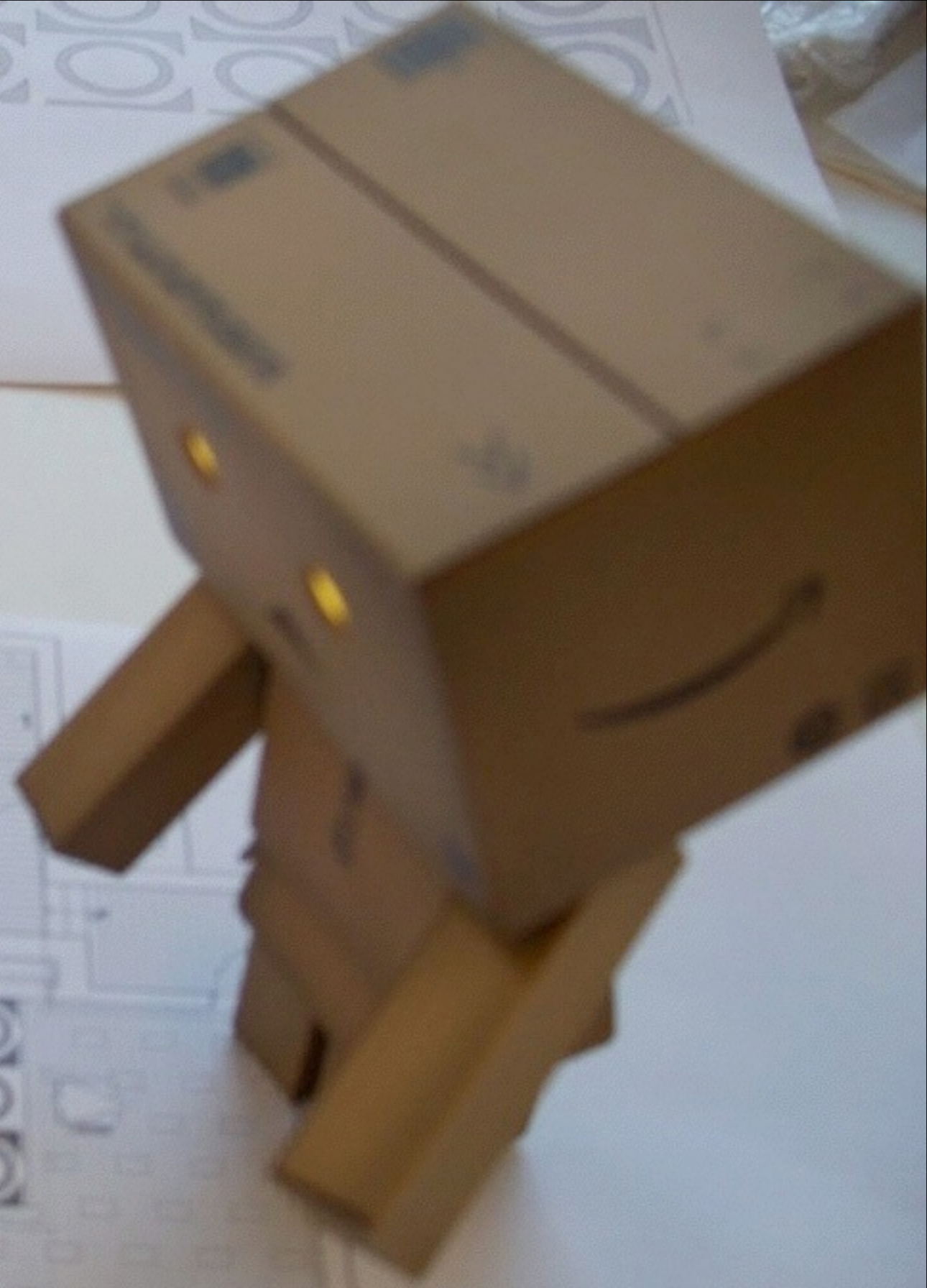
** for some definitions of innovation*



Not all lessons learned
are taught correctly

I am blank

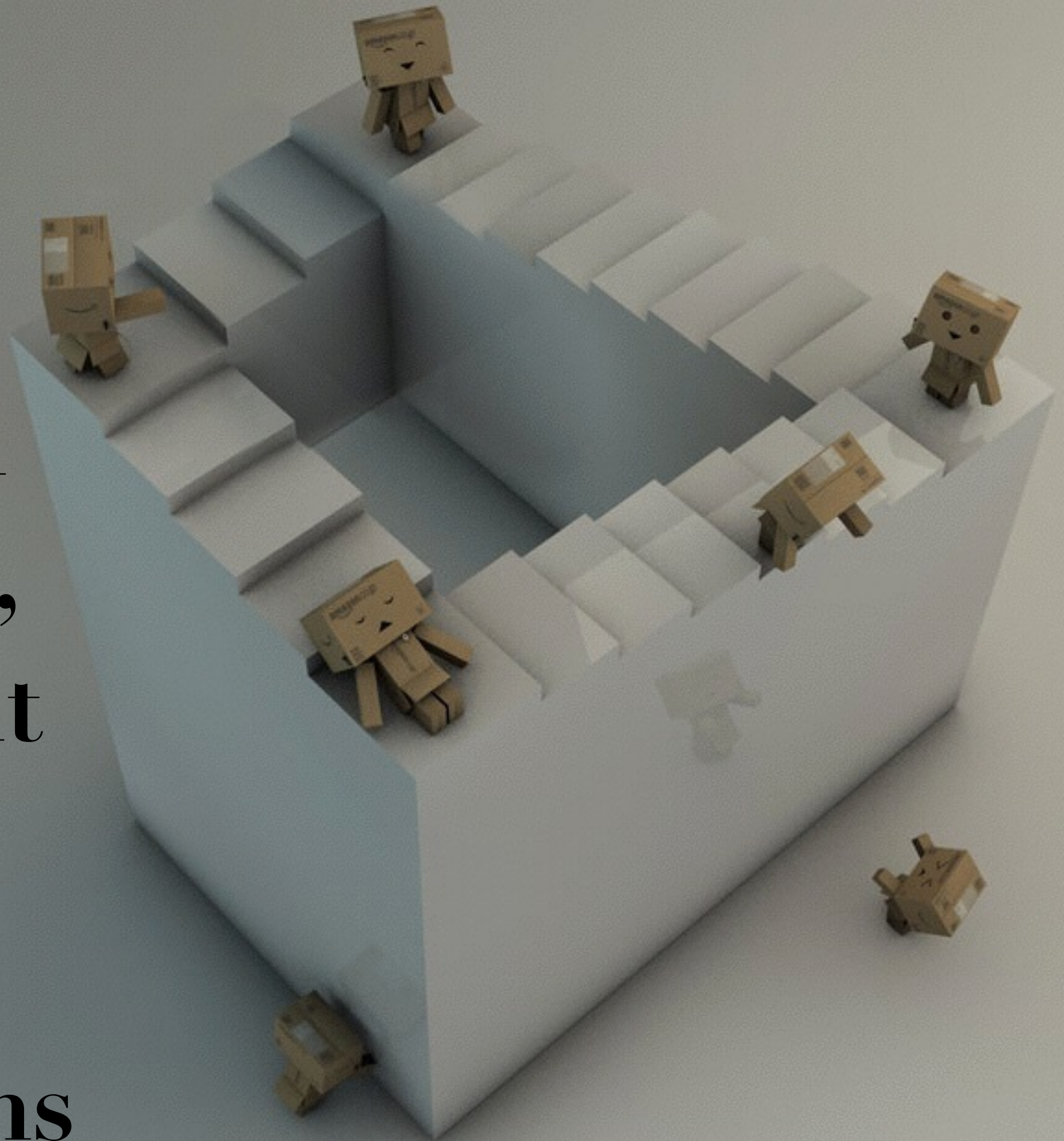
Caveat:
Science is hard



Story 1: ALL THE PHONES



when you
hardware,
you inherit
someone
else's
assumptions



hardware is
not magic

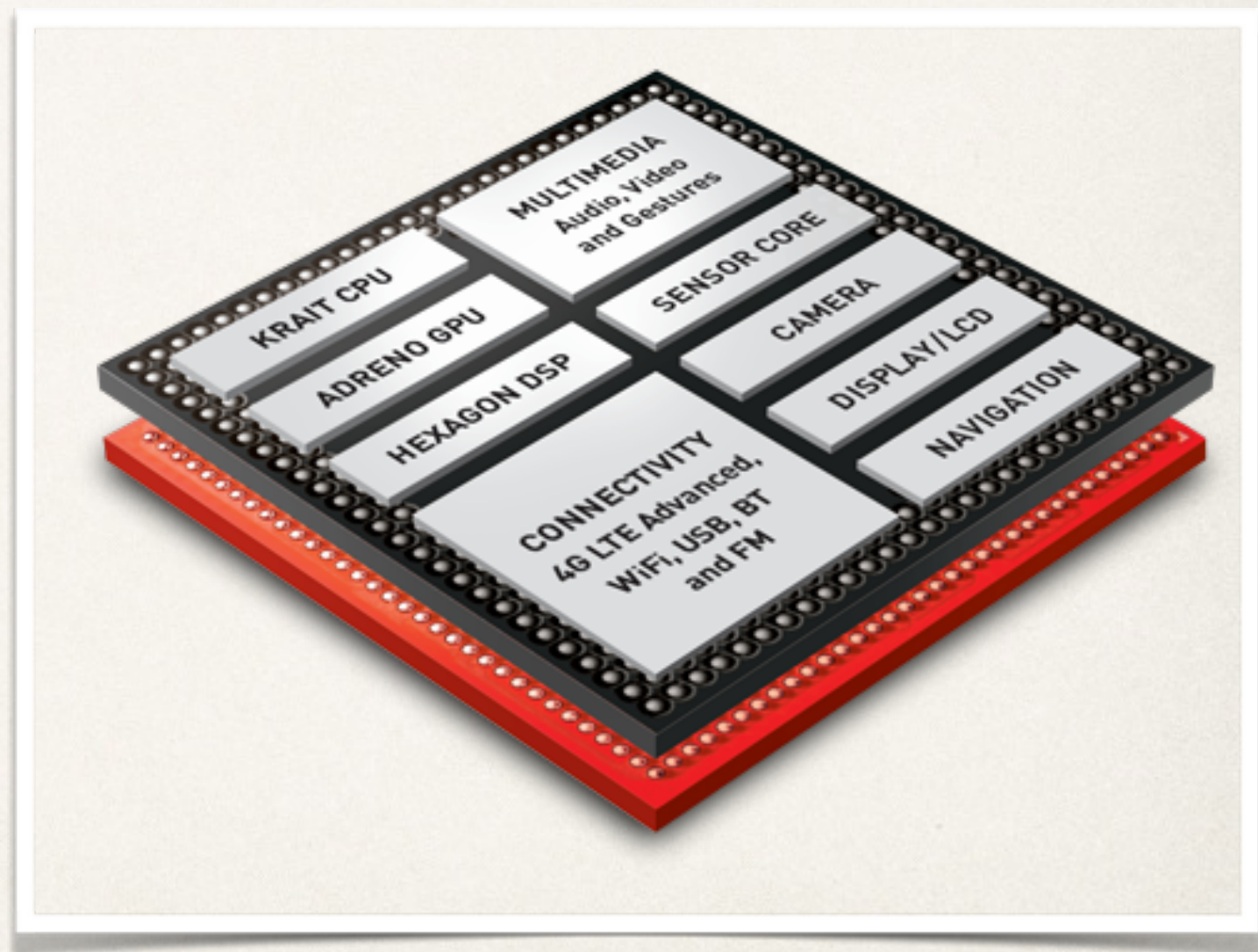




Hardware designers are
software people too!

Brand names are irrelevant

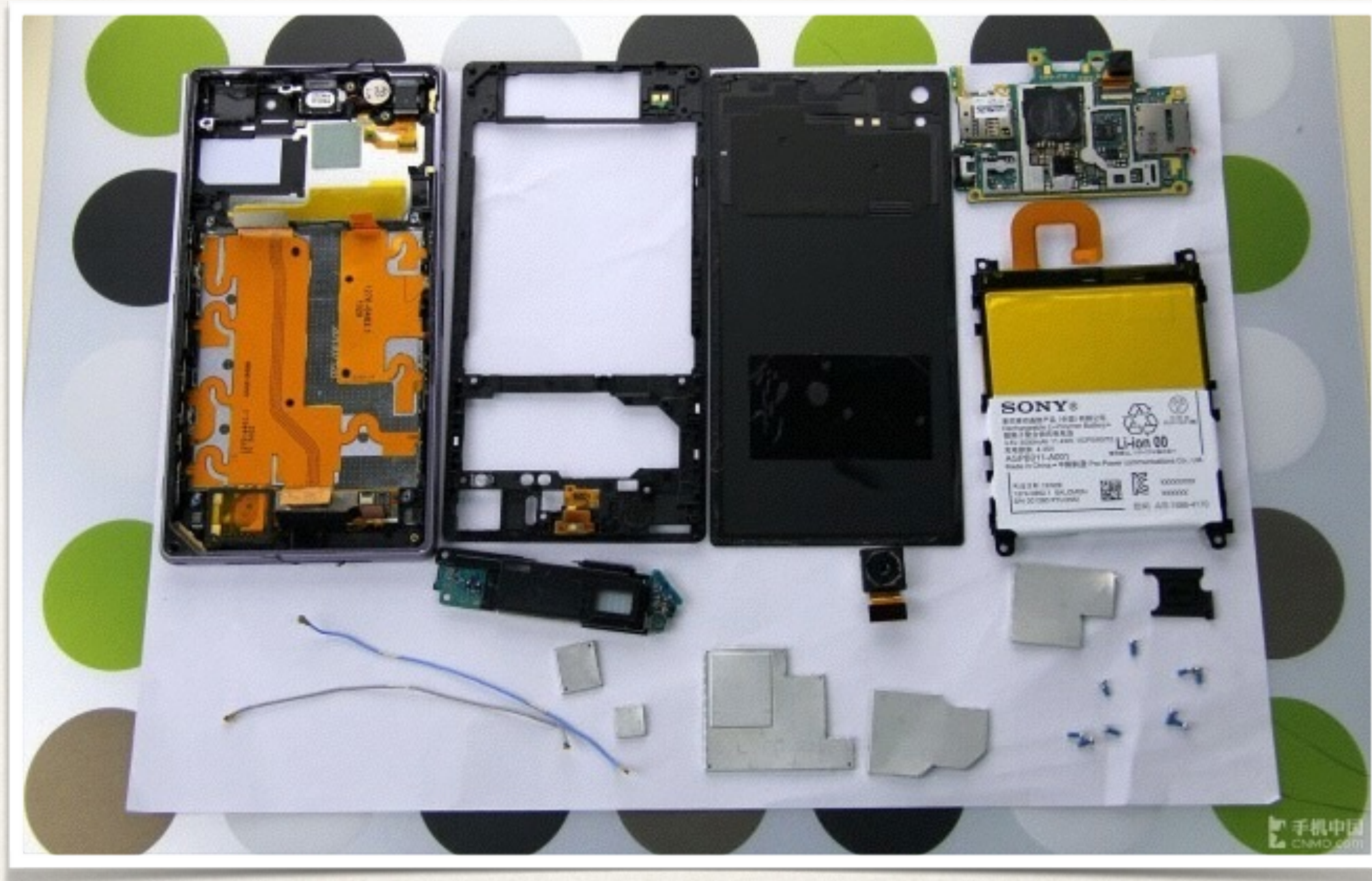
- ❖ Dirty little secret:
 - ❖ Qualcomm makes SoCs
- ❖ Dirtier little secret
 - ❖ Hardware people are lazy (just like software people)
- ❖ Dirtiest little secret:
 - ❖ Qualcomm makes a reference platform for smartphone designers





The Sony Xperia Z

The Sony Xperia Z Naked*



* Full Disclosure: Actually a Z1

Hmm... what else runs a S4 Pro?



Moto X by Motorola



Google Nexus 4

OK, and the S4 Plus?

Droid RAZR HD by Motorola



Samsung Galaxy S III



Nokia Lumia 1020

Ok, and the 600?

LG Optimus G Pro



Samsung GALAXY S4



HTC One

Ok, and the 800?



Sony Xperia Z1

Google Nexus 5



Samsung GALAXY Note 3

A common theme

A common platform

- ❖ Each vendor makes a phone
- ❖ Each phone is based on the SAME platform
- ❖ Each vendor adds special sauce
- ❖ Where there is a common platform, there is an SDK
- ❖ This is the gold standard reference on HOW to build a phone
- ❖ Why reinvent the wheel when you can reuse design and code?



Introducing: The meta phone

Snapdragon 800 MDP Mobile Development Platform - Smartphone & Tablet

The Snapdragon™ 800 Mobile Development Platform Smartphone (MDP/S) and Tablet (MDP/T) are essential tools for developers. These next-generation devices provides application developers and device manufacturers with early access to a high-performance Android™ 4.2 platform for development, testing and optimization of applications. Complete with asynchronous quad-core CPUs, these latest MDPs based on Qualcomm Technologies' Snapdragon 800 processor also includes an Adreno™ 330 GPU, Hexagon™ v5 QDSP6, and other advanced multimedia technologies.



So many specs

So much power

Tech Specs - Smartphone

NOTE: All features listed here may not be supported by the current version of software.

Processor

- Quad-core Krait 400 CPU at up to 2.3GHz per core
- Adreno 330 GPU
- Hexagon QDSP6 V5

Connectivity

- 802.11 n/ac Wi-Fi® 2.5GHz/5GHz, Bluetooth® 4.0, NFC

Display

- 4.3" (1280x720p) HD Multi-touch display

Memory

- 2GB 800MHz LPDDR3/32GB eMMC 4.5

Cameras

- Main: 12MP camera w/flash (1080P 30fps)
- Front: 2MP (1080p 30fps)

Audio

- Headset with ANC support
- 6 microphones and ultrasonic emitter for Fluence™ Pro and ultrasound pen & gestures

Sensors

- 3-axis accelerometer and 3-axis gyro
- 3-axis magnetometer (compass)
- Ambient light and proximity sensors
- Temperature and pressure sensors

Hard Keys

- Volume and zoom +/-
- Power on/off
- Screen rotation lock switch Back, Menu, Home and Search
- Reset (by pressing and holding the Power and Volume - buttons)

Connectors

- SuperSpeed USB 3.0, Micro A/B, with OTG 2.0 support (HDMI output via USB 3.0 connector (MHL))
- Hi-Speed 2.0 USB, Micro type B, device-only support
- MicroSD Card Slot
- 3.5mm headset jack with ANC support

so you want a meta phone?



[Services](#) [Products](#) [Solutions](#) [Resource Center](#) [Company](#)

[Bsquare](#) > [Bsquare-Store](#)

[Document Library](#)
[Software Downloads](#)
[Support Resources](#)

[Bsquare Store](#)

[Products Store](#)
[Toolkits Store](#)
[Training Store](#)

Shopping Cart

Qty.	Item	Price	Total	Remove
1	Snapdragon 800 Series-based Mobile Development Platform/Smartphone with Android	\$799.00	\$799.00	☐

[CHANGE](#)

Subtotal: \$799.00

[CONTINUE SHOPPING](#)

[CHECKOUT](#)

[EMPTY MY CART](#)

1 / (° - ° /) (/ ° □ °) / 0

From: "Florina Muntean" <FlorinaM@bsquare.com>
Date: Jun 27, 2013 2:04 PM
Subject: RE: BSQUARE Corporation Order Confirmation (#22041763)
To: "Josh "m0nk" Thomas" <monkworks.llc@gmail.com>
Cc:

Dear Josh,

Thank you for your Snapdragon (Tablet/Smartphone) order. Unfortunately, we must reject your order as Bsquare is restricted to sell this product only to mobile application development companies – no third parties, distributors, individuals or Qualcomm competitors. Being this order appears to be from a (3rd party, distributor, etc), we will be cancelling your order. Your credit card will not be charged.

Thank you!
Florina



The internet says welcome



<http://www.etsy.com/shop/sharpwriter>



HEUSER 2012

*** complaining about this has led to very cool Qualcomm people letting me know where else to order stuff. Thanks!**

BTW, the rest of this preso *might* violate the crap out of an NDA

all your assumptions are meta assumptions

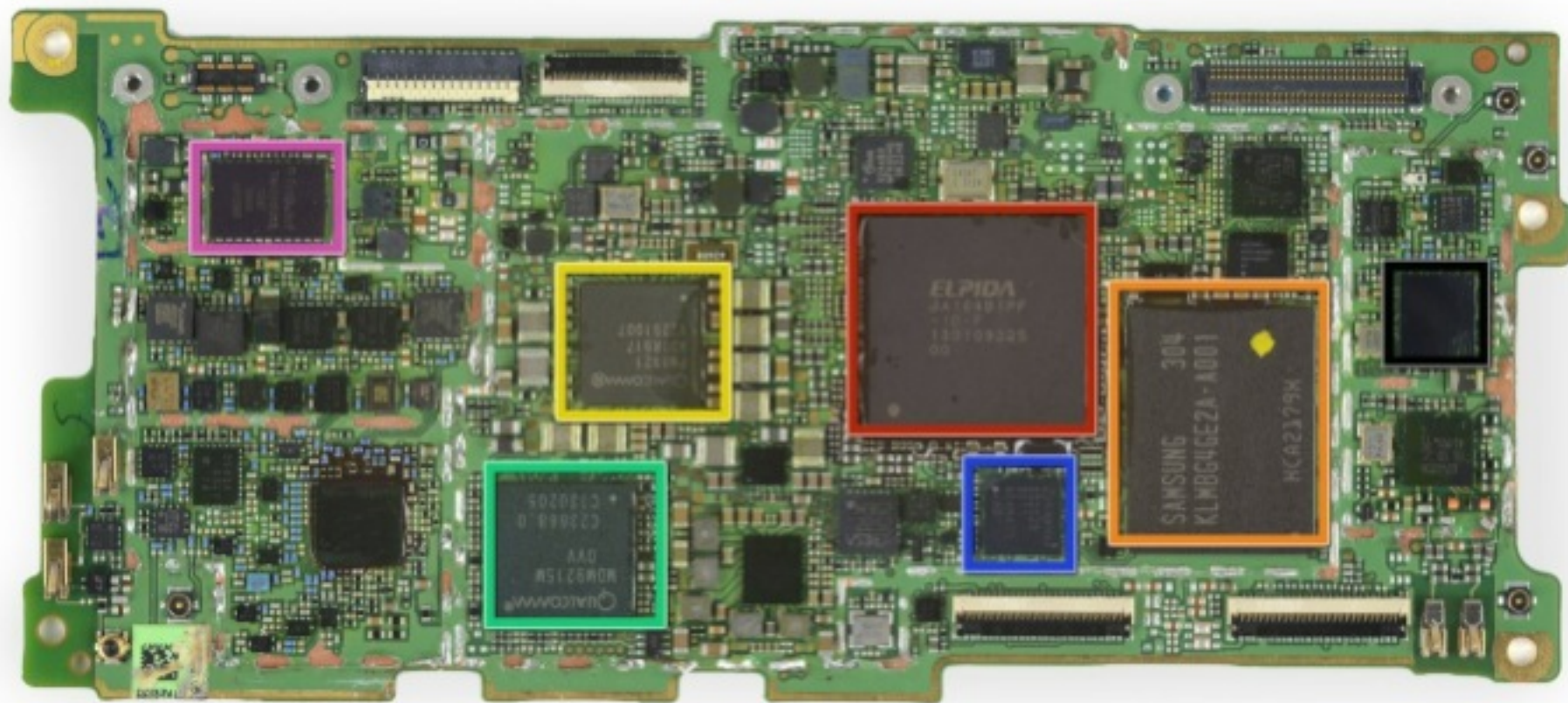
Random Desk Pron



Random Desk Pron



Random Desk Pron



My typical desk





moar!

extra phones?





Exploit the dev platform...
pwn the world?



I am blank

Story 2: Hardware is...



Project Burner:

High level overview

- ❖ Hypothesis:

- ❖ Given full kernel control of an Android phone, I can control the power and voltage from the internal battery to physically manipulate internal hardware. I can control the process and target individual components to the point of full kinetic destruction using unexpected voltages.

- ❖ End result:

- ❖ Hypothesis is correct. (kinda?)

Project Burner:

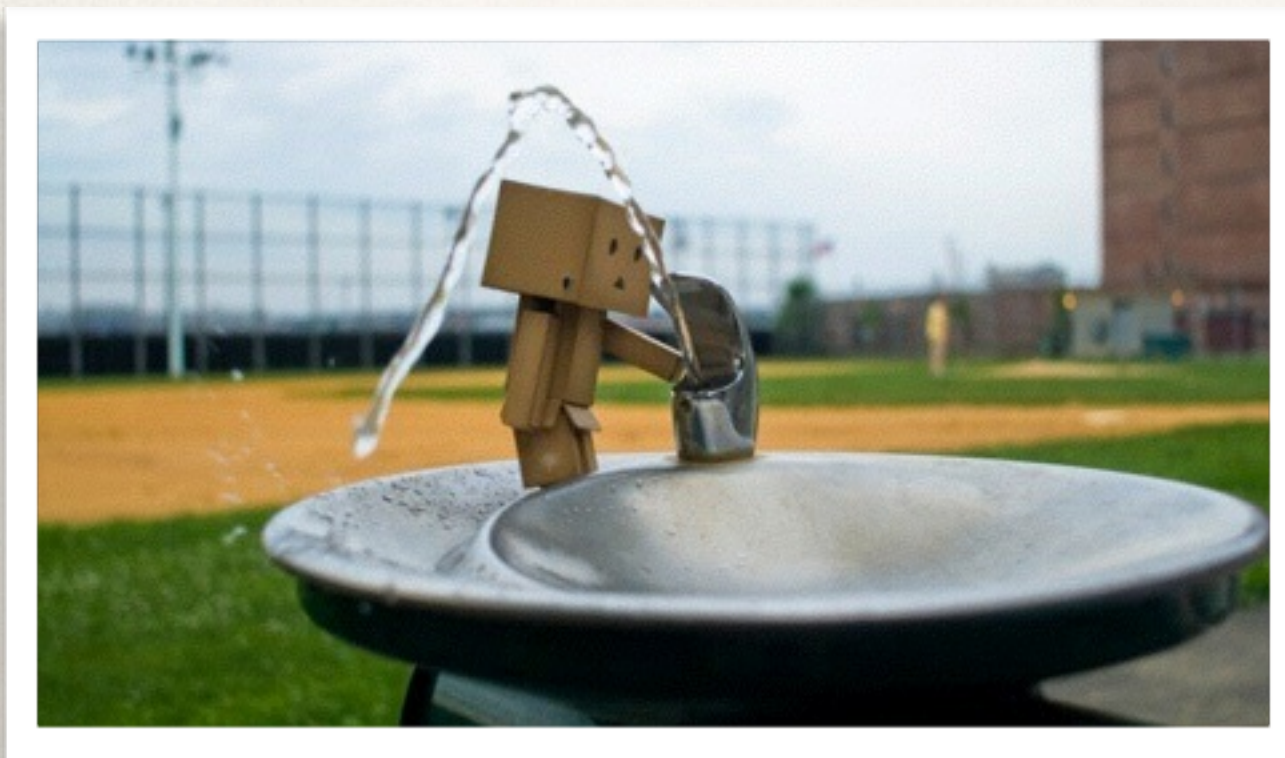
Android Power Hardware

- ❖ The Battery stores raw power to distribute
- ❖ The USB stack also pushes power into the system
- ❖ The PMIC hardware is utilized to distribute voltage across the traces
- ❖ Kernel manages the PMIC settings directly
- ❖ Not all traces are protected by capacitors and resistors



Project Burner:

Android Power Regulation



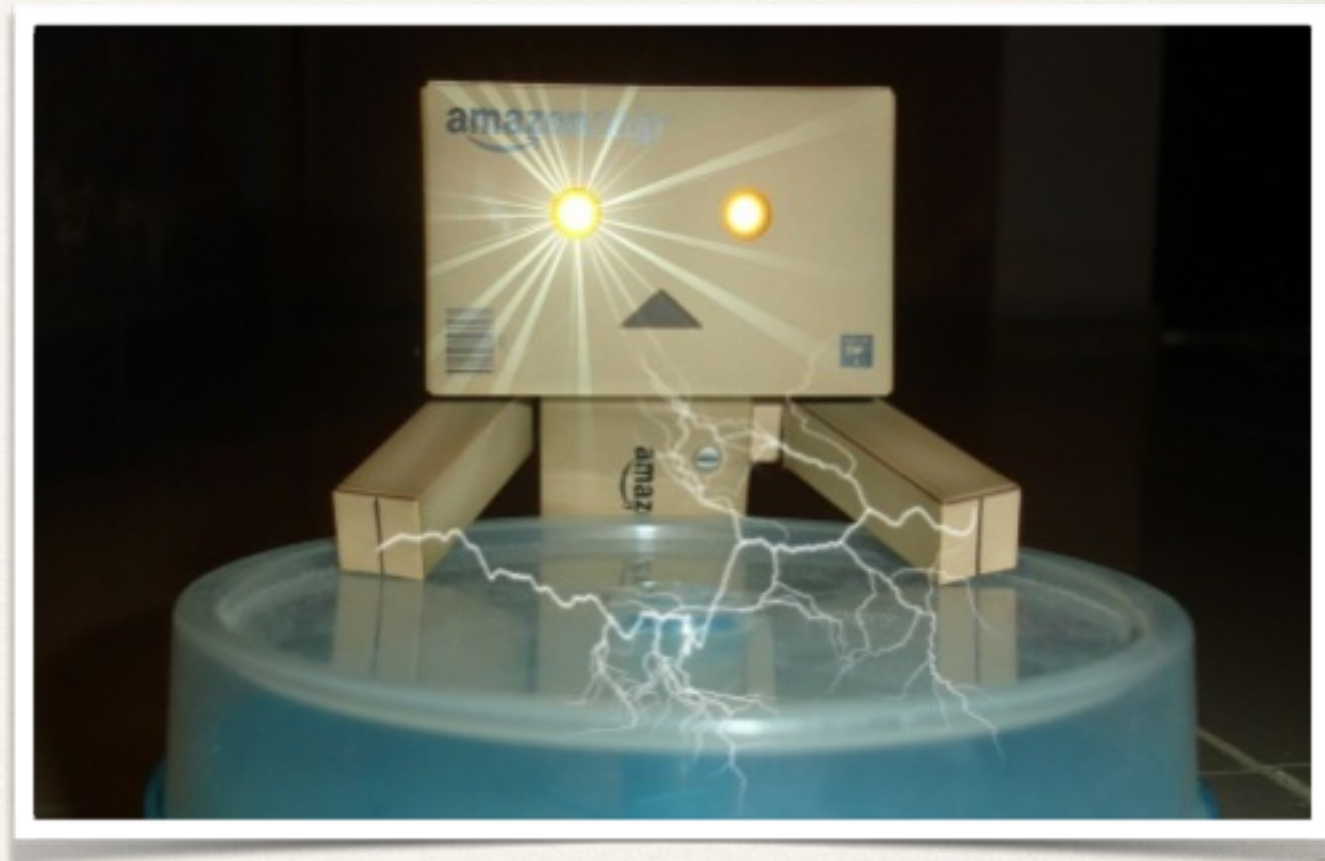
- ✧ Well documented in:
 - ✧ `<kernel_source>/Documentation/power/regulator/overview.txt`
- ✧ Aside from drivers, less than 10 *.c and *.h files control the voltage flow throughout the PCB
- ✧ Of particular interest is the *_regulator.c file for whatever PCB you are exploring



Without docs

Blind this research was

- ❖ Our vendor of interest does not like to release “real” documentation to the public
- ❖ When I started this, I did not have the “leaked” docs
- ❖ FWIW, I would do it slightly different today



Project Burner:

The target

- ❖ The target platform for Project Burner was the Sony Xperia Z (yuga)
- ❖ Based on the Qualcomm Snapdragon reference platform





Project Burner: Thermal regulation

Project Burner:

Thermal regulation

- ❖ When playing with voltages out of expected ranges, one needs to pay attention to the thermal checking daemon: thermald
- ❖ This daemon should not be shut down, it simply needs to be nullified
- ❖ Don't forget, there are multiple thermal sensors on the phone... gotta catch 'em all.



Project Burner:

Thermal Fun

```
...
...
//      L13 runs at: 1740000 / 1740000
// ** **
// ** ** m0nk: therm sounds interesting... _adc does as well <-- poke hard here
// ** **
L13 =      "8921_l13"          NULL
          "apq_therm"        "pm8xxx-adc"

//      L14 runs at: 1800000 / 1800000
// ** **
// ** ** m0nk: therm sounds interesting... _adc does as well, as does CHARGER <-- poke
hard here
// ** **
L14 =      "8921_l14"          NULL
          "vreg_xoadc"        "pm8921-charger"
          "pa_therm"          "pm8xxx-adc"

...
...
```


Project Burner:

Thermal regulation



- ❖ We can not fry the Thermal system directly
- ❖ We can overvolt and corrupt the output
- ❖ We can “tweak” the values and somewhat control / manipulate thermal readings

Project Burner: Attacking the SoC



Project Burner:

The Qualcomm SoC target

- ❖ #ResearchFail
- ❖ The main krait cores fight back hard against bad voltages
- ❖ Internal to SoC protections work*
- ❖ Anything extreme simply goes unstable and reboots



Project Burner: The Qualcomm SoC target

Cancel all my meetings.

Someone on the internet
is wrong.



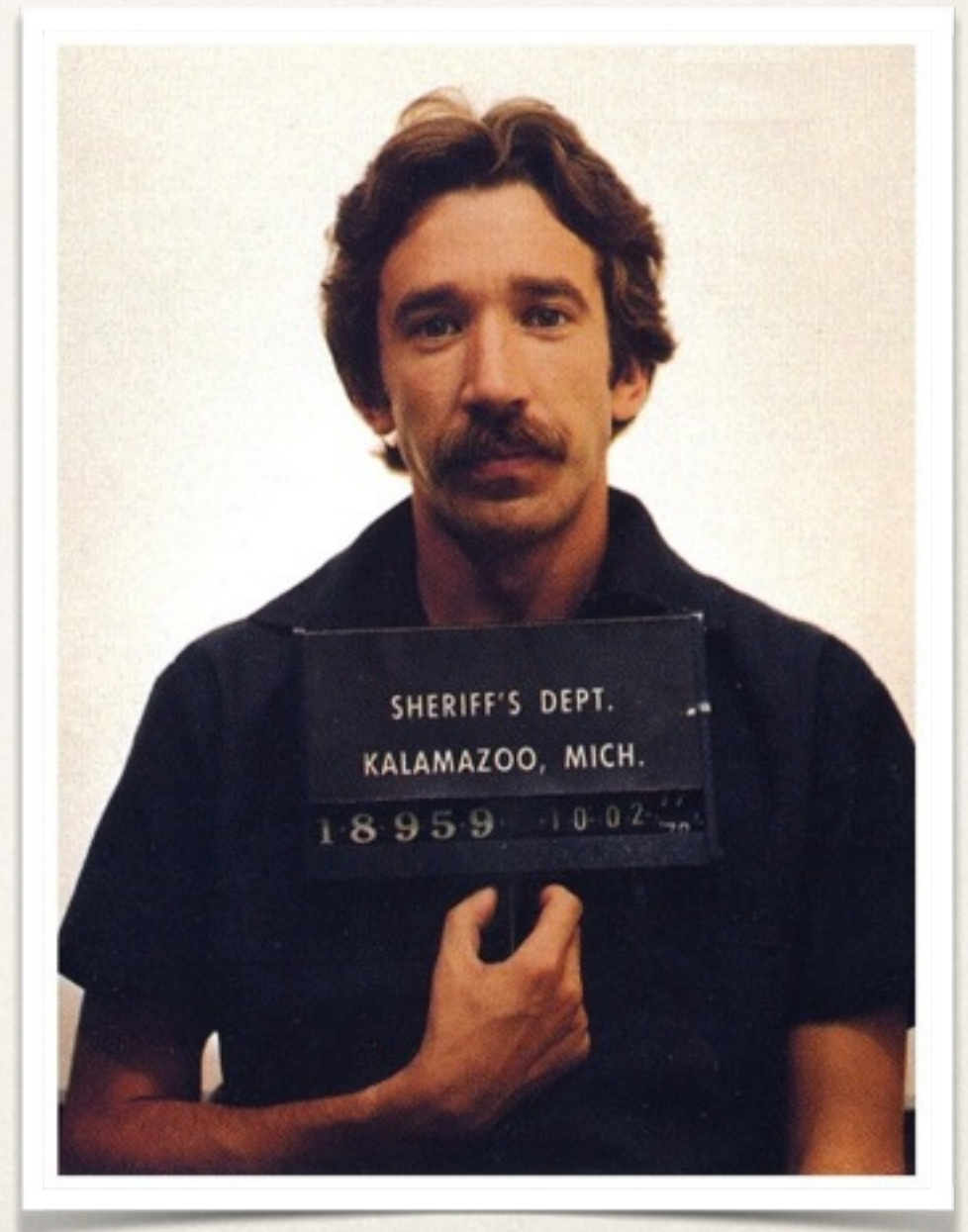
someecards.com

- ❖ That guy on the internet that warns you to not overclock or your phone will immediately burst into flame? He is a damn liar.
- ❖ Source code looks a lot like an overclock to 6.66Ghz

Project Burner:

Never Give Up, Never Surrender?

- ❖ Did you know you can tell the kernel to fail the USB stack?
- ❖ Did you know you can tell the kernel to extreme overclock?
- ❖ Did you know this uses power?
- ❖ Did you know without USB you can't get more power?





1 phone down
platform: 1 / josh: 0.5



Project Burner: Attacking NAND

Project Burner:

The NAND target

- ❖ The target platform for Project Burner was the Sony Xperia Z (yuga)
- ❖ Based on the Qualcomm Snapdragon reference platform
- ❖ The NAND controller is tied to the SDCard controller
- ❖ Qualcomm MSM 7X00A SDCC controls both traces on the PCB



Project Burner:

Upping NAND Voltage

```
project kernel / sony / apq8064 /
```

```
diff --git a / arch / arm / mach-msm / board-sony_yuga-regulator.c  
      b / arch / arm / mach-msm / board-sony_yuga-regulator.c
```

```
-- RPM_LDO(L5, 0, 1, 0, 2950000, 2950000, NULL, 0, 0),
```

```
++ RPM_LDO(L5, 0, 1, 0, 5900000, 5900000, NULL, 0, 0),
```

```
-- RPM_LDO(L6, 0, 1, 0, 2950000, 2950000, NULL, 0, 0),
```

```
++ RPM_LDO(L6, 0, 1, 0, 5900000, 5900000, NULL, 0, 0),
```


Project Burner:

Upping NAND Voltage



- ❖ With higher voltages:
 - ❖ Every NAND read corrupts the data in transit
 - ❖ Every NAND write corrupts the NAND hardware
- ❖ PMIC values are stored so rebooting the device essentially corrupts all of NAND as the bootloader tries to load the kernel

Project Burner:

Dropping NAND Voltage

```
project kernel / sony / apq8064 /
```

```
diff --git a / arch / arm / mach-msm / board-sony_yuga-regulator.c  
      b / arch / arm / mach-msm / board-sony_yuga-regulator.c
```

```
-- RPM_LDO(L5, 0, 1, 0, 2950000, 2950000, NULL, 0, 0),
```

```
++ RPM_LDO(L5, 0, 1, 0, 1250000, 1250000, NULL, 0, 0),
```

```
-- RPM_LDO(L6, 0, 1, 0, 2950000, 2950000, NULL, 0, 0),
```

```
++ RPM_LDO(L6, 0, 1, 0, 1250000, 1250000, NULL, 0, 0),
```


Project Burner: Dropping NAND Voltage

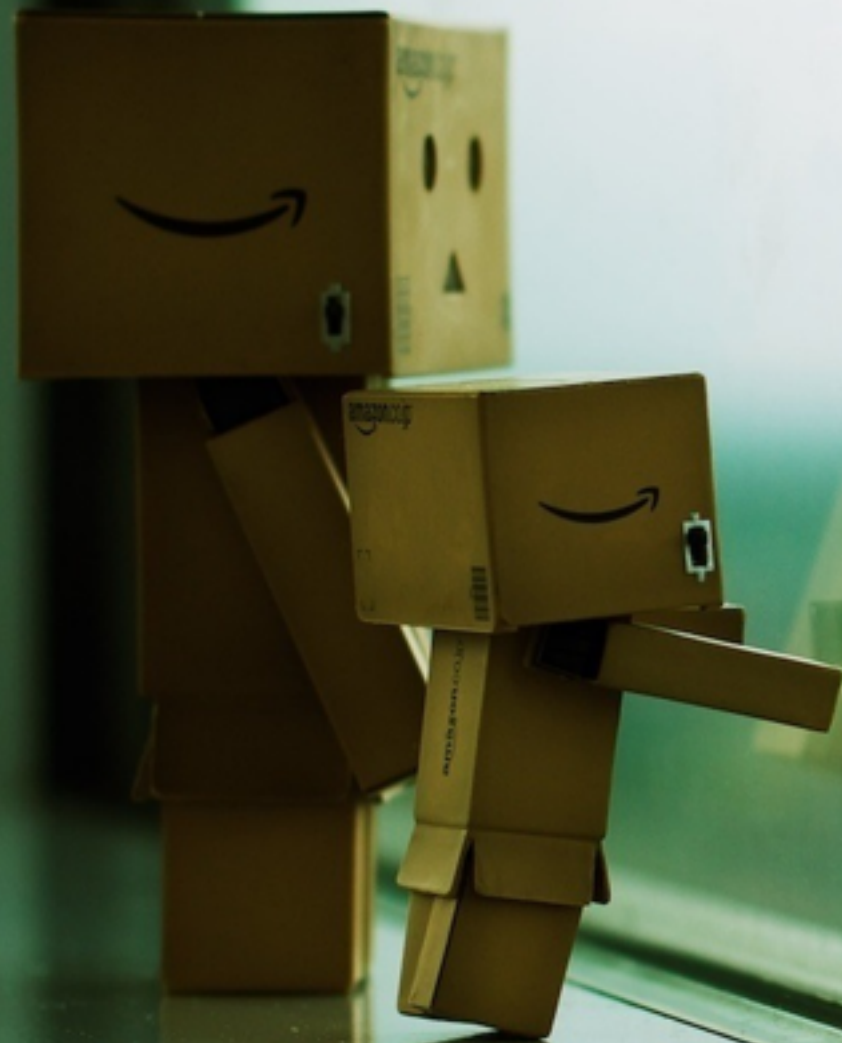
- ❖ With lower voltages:
 - ❖ Most NAND reads corrupt the data in transit
 - ❖ Every NAND write attempt fails at the hardware level
- ❖ This technique essentially generates a phone frozen in time, no writes can occur and the device fails to successfully boot





**2 phones down
platform: 1 / josh: 1.5**

Project Burner: Attacking WiFi



Project Burner:

The WiFi target

- ❖ Part of the SoC, but appears to have BGA pins for direct external access
- ❖ Regulators L4, L10 and S2 used on the board
- ❖ Other config in the driver itself:
 - ❖ `wcnss_riva.c`

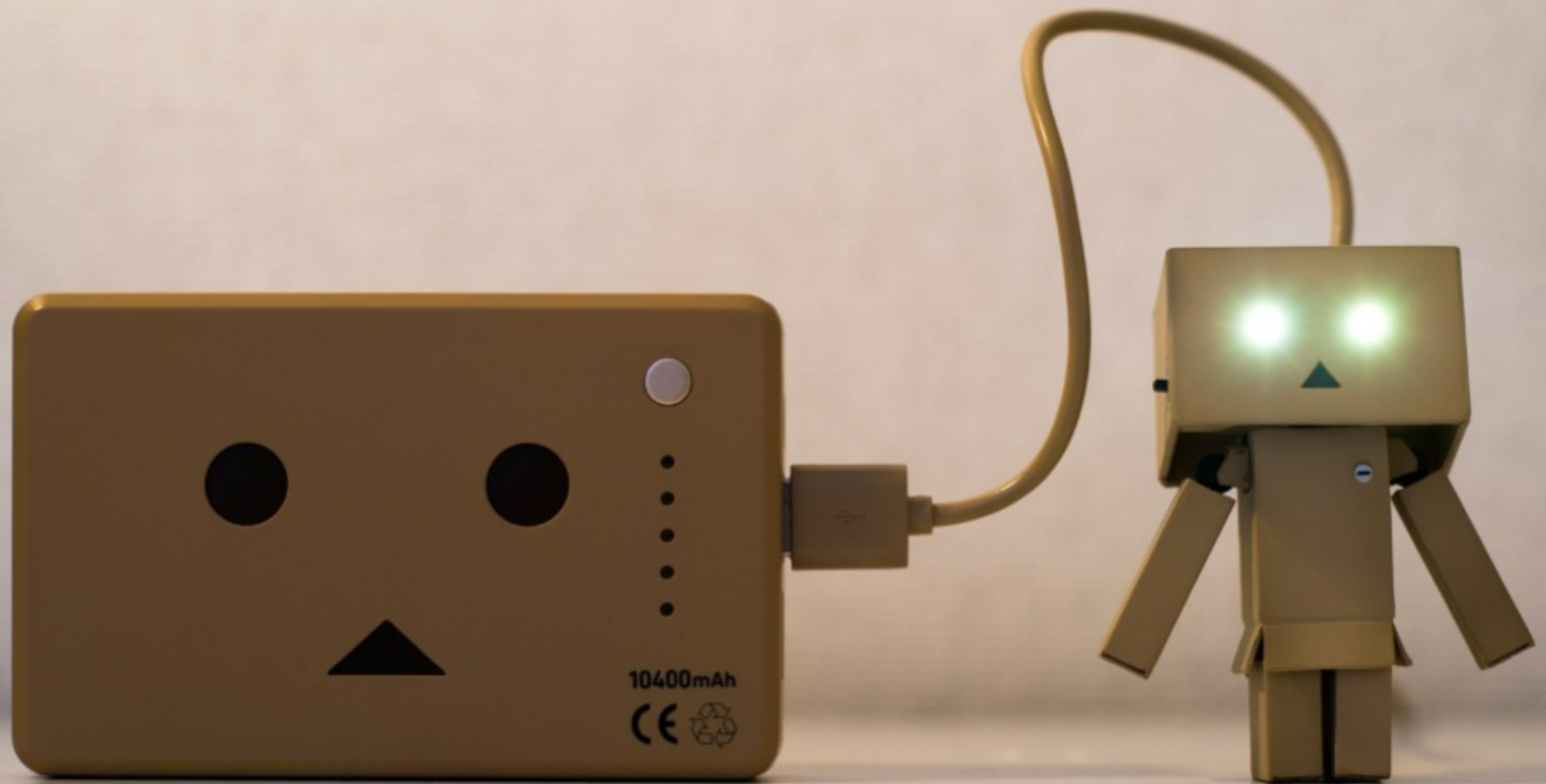


Project Burner:

The WiFi target



- ❖ Protected in SoC, can not fry it
- ❖ Can edge up on over volting to corrupt data in transit



Project Burner: Attacking USB

Project Burner:

The USB Stack target

- ❖ Finally, we have to start adjusting PMIC values and GPIO values directly
- ❖ Fun with OTG?
 - ❖ Sony does better than most here



Project Burner:

The USB Stack target



- ✧ Corrupt Values
- ✧ Disable Charging
- ✧ Push more voltage than expected over OTG
- ✧ #NoFire

Project Burner: Attacking the Power Plane (& other things)



Project Burner:

The Power Plane target

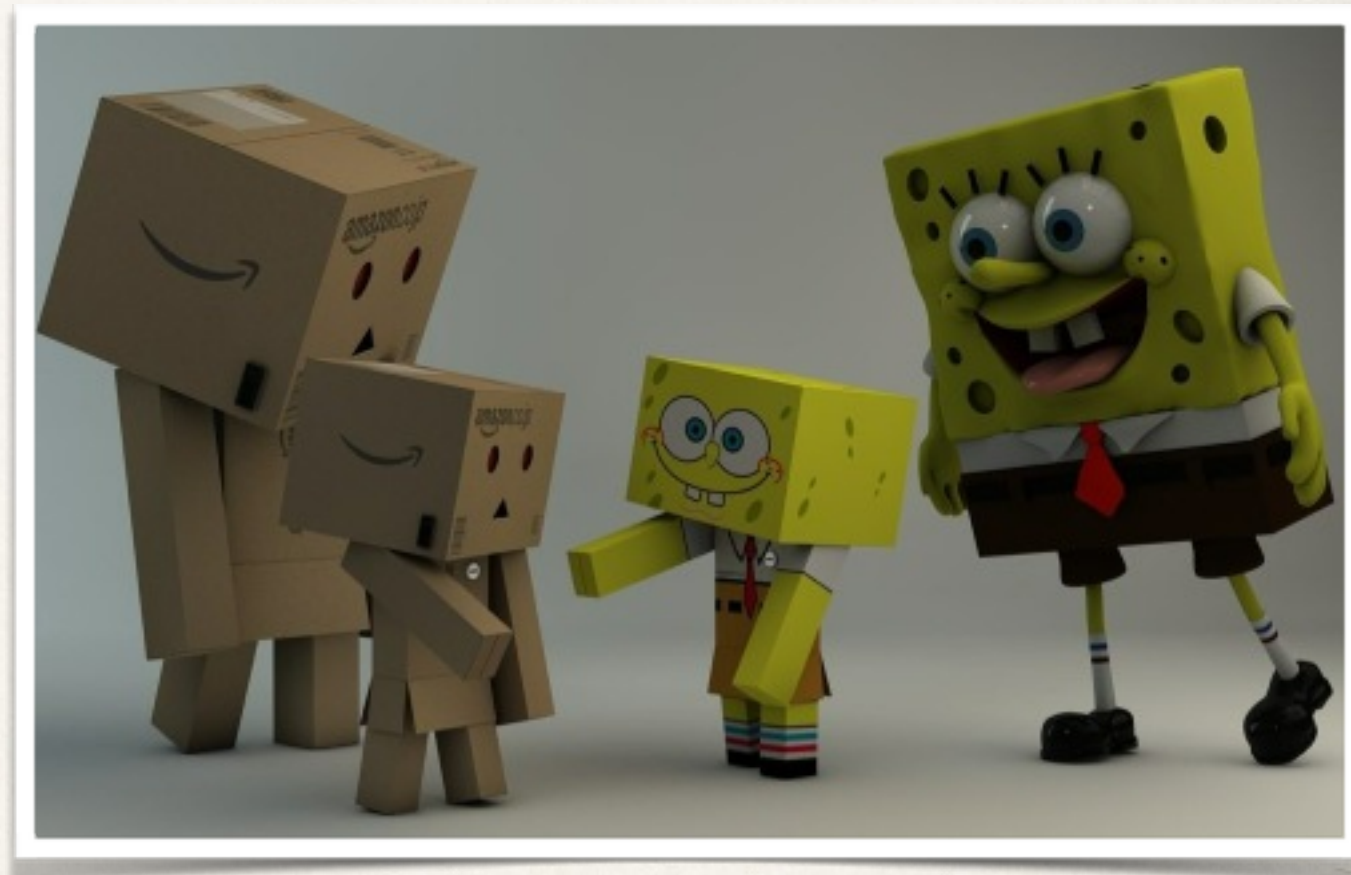
- ❖ Everything needs power
- ❖ Reference power is on a plane in the PCB
- ❖ Up that?
- ❖ Things broke, not a clue as to what it was



Project Burner:

The Small Things target

- ❖ Attacked the Screen
 - ❖ Nothing of Real Interest :(
- ❖ Attacked the Camera
 - ❖ Nothing of Real Interest :(
- ❖ Attacked Audio Hardware
 - ❖ Nothing of Real Interest :(
- ❖ Attacked Hexagon Hardware
 - ❖ Need more time / info here...





3 phones down
platform: 4 / josh: 2.5

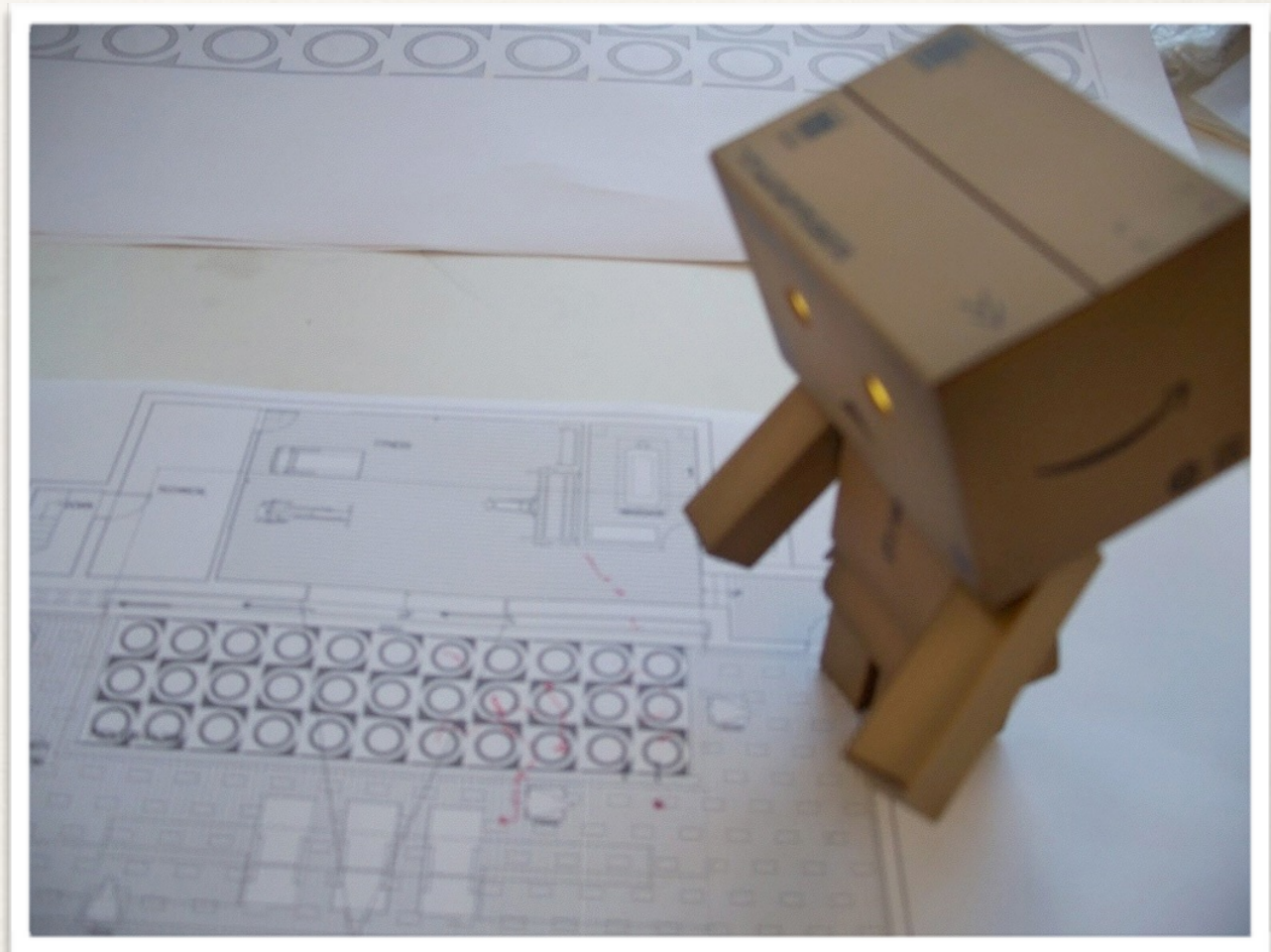
Project Burner: Attacking Battery



Project Burner:

The Battery target

- ❖ This was hard (more in a second on this)
- ❖ Battery got very hot
 - ❖ Overly complex way to heat the glue on the phone for disassembly
- ❖ Never able to fully boot with this setup, lots of loops
- ❖ Ran overnight (in garage)



Project Burner:

The Battery target



- ❖ Technically able to recover phone
- ❖ Phone never really functioned again?

4 phones down
platform: 7 / josh: 3.5

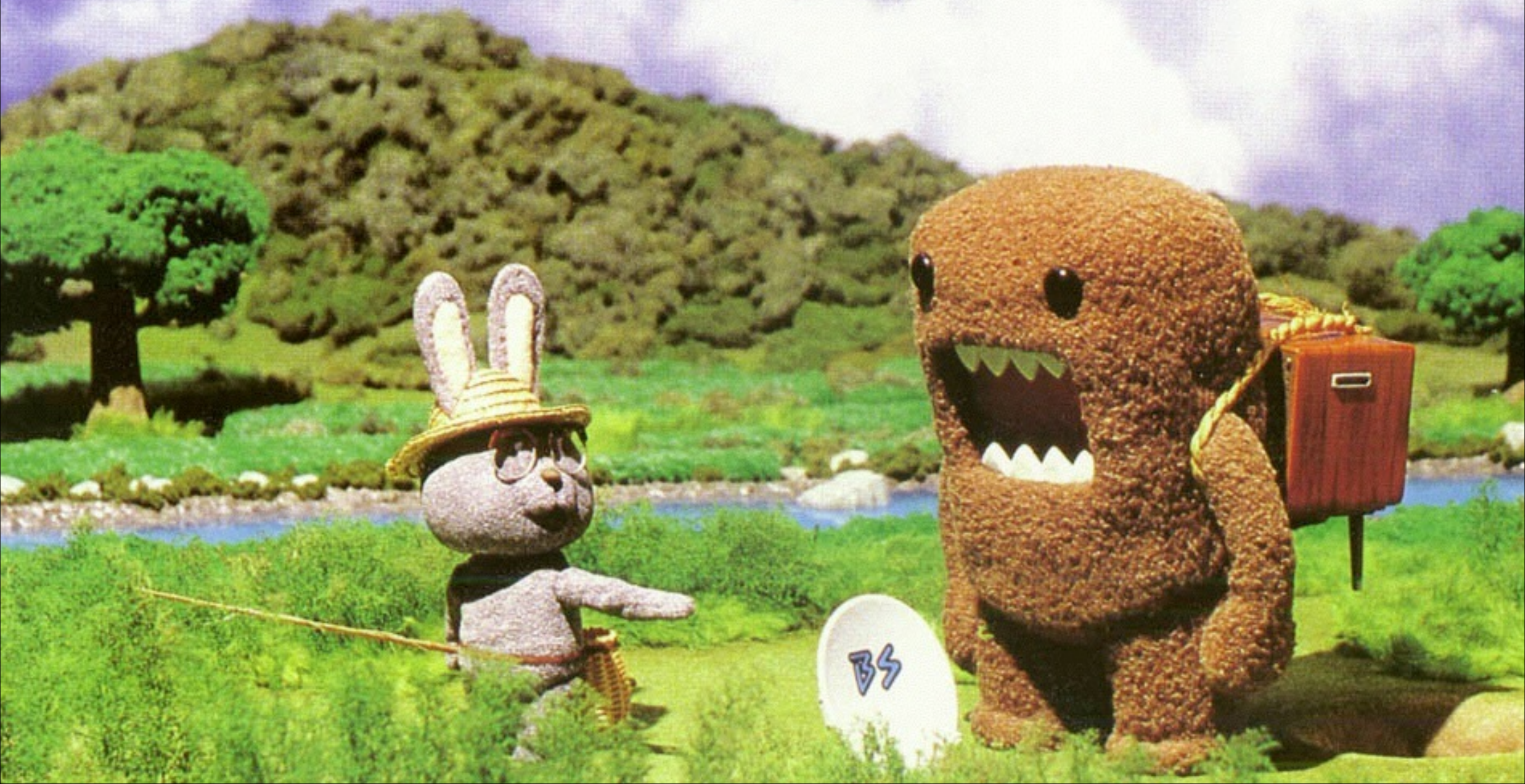


Project Burner:

The Battery target

- ❖ Turn off all Thermal Checks
- ❖ Turn off all Voltage Failsafe Checks
- ❖ Turn off all Capacity Failsafe Checks
- ❖ Turn off the ability for the battery to report 100% charged
- ❖ Turn off the ability to move out of “Fast Charging” state
- ❖ More headaches, see Doc page 62

Please read the paper
github.com/monk-dot/ProjectBurner



I am blank

Story 3:
MOAR MEMES
&
thx





I'm in your
hardware

*I am your
hardware*



If this interests you, help me
continue the exploration...





Questions?



Thank You - @m0nk_dot